



Online Safety Policy 2021/2022

To love, to serve and learn.

We are a school family journeying together in God's love.
We serve each other to achieve our best.
We learn in fun and creative ways,
respecting everyone's gifts.

Policy Details

Policy Date: **September 2021**

Policy Status: **Statutory**

Policy Review Cycle: **Annual**

Next Review Date: **September 2022**

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. St Edward's Catholic Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

Links to other policies and national guidance

The following school policies and procedures should also be referred to:

- Safeguarding Policy
- Whistleblowing policy
- Behaviour Policy
- Staff code of conduct
- Data Protection
- Social Media and Digital Photography Policy
- Distance Learning Policy

The following local/national guidance should also be read in conjunction with this policy:

- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE 2021
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

Roles and Responsibilities The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors: Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher: Responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Subject leader who is also the E-Safety Co-ordinator.

- Must ensure they undertake regular training and make sure and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant- and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Subject Leader / E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff

- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors

Technical staff: The ICT Technician is responsible for ensuring that:

- monitoring software and systems are implemented and updated as agreed in school policies

Teaching and Support Staff: Teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- digital communications with pupils (email / Learning Platform - DB Primary) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection / Child Protection Officer: Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Teaching and Learning

The internet and other technologies are embedded in our pupils' lives, not only in school but at home also, and we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a curriculum and lessons which have e-Safety related lessons embedded throughout.
- We will celebrate and promote e-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons, including:
 - the need to protect personal information
 - considering the consequences their actions may have on others
 - the need to check the accuracy and validity of information they use
 - the need to respect and acknowledge ownership of digital materials.

- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- School will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Remote/Home Learning - Please refer to the 'Distance Learning Policy'.

Response to an incident in school or online

- At every stage the child should be involved in or informed of the action taken. Parents will be informed.
- Urgent or serious incidents should be referred straight to the head teacher and if necessary, refer to the other related internal policies e.g. Anti-Bullying, Child Protection, Social Media and Digital Photography policies.
- Normal recording systems on CPOMS should continue. Entries should be factual and action/follow up recorded also.

Staff Training - Our staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise.

- As part of the induction process all staff receive information and guidance on the Acceptable Use Policy , e-security and reporting procedures.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing ICT Systems and Access The school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive

- All users will be made aware of the 'acceptable use' of IT equipment (appropriate to their age and type of access). Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT system and that such activity will be monitored and checked.
- Pupils will access the network using an individual username and a class password which the teacher supervises.
- All internet access will be undertaken alongside a member of staff or, if working independently a member of staff will supervise at all times.
- Members of staff will access the internet using an individual ID and password, which they will keep secure and they will ensure that they log out after each session and not allow pupils to access the internet through their ID or password. They will abide by the school AUP at all times.

Managing Filtering

- The school has a 'filtering' system in place which is managed by the school and Brindley Data Services Banned phrases and websites are identified.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Co-ordinator immediately.
- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safety Co-ordinator. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).
- Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the headteacher/e-Safety Co-ordinator prior to being released or blocked.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

E-Mail

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers.
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails.
- Irrespectively of how pupils or staff access their school email (from home or within school), school policies still apply.
- Chain messages are not permitted or forwarded on to other school owned email addresses.

Social Networking Please see the Social Media and Digital Photography Policy.

Pupils Publishing Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.
- Written permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use personal portable devices to store images/video/sound clips of pupils.

Mobile Phones and General use of Personal Devices Please see the Social Media and Digital Photography Policy.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

General Data Data Protection (GDPR) and e-safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

Personal and sensitive information should only be sent by e mail when on a secure network. Personal data should only be stored on secure devices.

In the event of a data breach, the school will notify the Trust's Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

Support for Parents

- Parents attention will be drawn to the school's e-Safety policy and safety advice in newsletters, the school website and e-Safety information workshops.
- The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.
- Parents are expected to abide by the Social Media Code of Conduct for Parents and Carers.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/Safeguarding Co-ordinator). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

Sexual Harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our school follows and adheres to the national guidance - UKCCIS: *Sexting in schools and colleges: Responding to incidents and safeguarding young people*

Responses to Incident of Concern

An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an e-Safety nature on CPOMS.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy. The school also reserves the right to report any illegal activities to the appropriate authorities

ICT Subject Leader - Mrs Tomlinson
Designated Safeguarding Lead: Mrs Snell
Safeguarding Governor - Vicky Hoare

Policy Review Date: September 2022 or when changes are necessary to comply with school policy or national legislation.

Acceptable Use of the Internet Policy and Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for students/volunteers to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- all adults will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- all adults are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that adults will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect students/volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- ❖ I understand that the St Edward's Catholic Primary School will monitor my use of the school digital technology and communications systems.
- ❖ I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- ❖ I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- ❖ I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- ❖ I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using St Edward's Catholic Primary School's ICT systems:

- ❖ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- ❖ I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- ❖ I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- ❖ I will not use my personal equipment to record these images, unless I have permission to do so. *Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.*
- ❖ I will only use social networking sites in school in accordance with the school's policies.
- ❖ I will only communicate with students / pupils and parents / carers using official school systems and any such communication will be professional in tone and manner
- ❖ I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the St Edward's Catholic Primary School:

- ❖ When I use my mobile devices (laptops / tablets / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- ❖ I will not use personal email addresses on the school ICT systems without seeking permission.
- ❖ I will not use USB devices whilst at the school.
- ❖ I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- ❖ I will ensure that my data is regularly backed up, in accordance with relevant school / policies.
- ❖ I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- ❖ I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- ❖ I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- ❖ I understand that data protection policy requires that any pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- ❖ I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- ❖ I will ensure that I have permission to use the original work of others in my own work
- ❖ Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- ❖ I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- ❖ I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the trust/university and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name :

Position in school:

Signed:Date: